THOMSON REUTERS
WHY YOU SHOULD WORRY ABOUT OPERATIONAL RISK

A THOMSON REUTERS WHITE PAPER

Thomson Reuters are leaders in the provision of information, trading and technology solutions to market participants and as a core infrastructure provider we have a strong interest in actively contributing to the debate around the future shape of financial markets. Thomson Reuters has led and will continue to lead change in the financial markets, responding to both regulators and customers by providing solutions in the post-regulatory world.

Date of issue: December 2012

INTRODUCTION

The regulatory landscape is changing.

Basel III in particular will have a significant impact on all aspects of the banking sector. We are already seeing significant increases in both the quality and quantity of capital that is required to be set against the wider risks of running a business but the wider regulatory policies also seek to improve the underlying risk-management capabilities of banks, whether looking at Legal, Operational, Market, Regulatory or Credit Risks.

"I have seen a disturbing uptick in what we call operational risk,"

Federal Reserve Governor Sarah Bloom Raskin, 16th October 2012

Many banks and other key financial institutions have balked at the costs involved in the increased capital requirements and in complying with the broad risk management requirements of Basel III, however Basel II introduced the three pillar concept and recognised the importance of strong Operational Risk management by including this within pillar 1. Basel III has continued in this vein with the proposed pillar 2 focus on risk management.

Whilst supervisors everywhere are increasingly sensitive to the balance which has to be achieved between cost pressures and ensuring that banks take operational risk seriously; there is a major focus on avoiding the risk of "black swan" or "fat tail" events; which could further jeopardise financial stability. Compliance and risk management are no longer simply a question of aligning with best practice through a team located somewhere in the institution. Risk appetite should be established and set at Board level, taking into account shareholder and regulators' expectations. The concept of 'enterprise risk management' is now well-established. ***This paper will highlight some less considered elements of operational risk and demonstrate how a different approach can lead to real benefits to the business***. Managing operational risk is now bang square in the middle of the business – and the cost of failure carries significant regulatory, financial and reputational consequences.

So what is operational risk?

"Operational risk management began to emerge in banks as a distinct discipline and term of art in the early 1990's. They had begun to realise that they were as likely to be brought down by failures of process and systems or the behaviour of their employees, or indeed by external events, as they were by bad debts and credit risk which, to that date, had been seen as their primary risk, along with market risk, and was what, effectively, the head of risk's job was all about. Interestingly, the event which captured their attention initially and which featured at every operational risk conference at the time was the Piper Alpha disaster in 1988 when 167 people lost their lives of the 226 who were on the rig. The reasons for that disaster were failures of communication regarding the safety status of pumps, lack of safety refuges and procedures, minimum compliance with safety regulations and, frankly, weak regulation driven largely by national political and economic imperative. Plus ça change, when we consider Deepwater Horizon. And all operational risks.

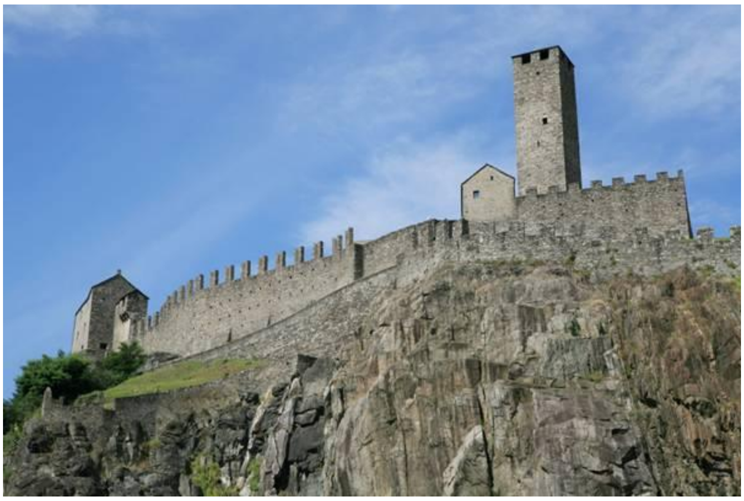
But the game-changing year for financial markets was 1995, the year of Nick Leeson at Barings and the rogue trading scandals at Daiwa Bank and Sumitomo Corporation. Operational risk was headline news.

Indeed, if you look at events which have threatened the global financial system in various ways in recent years: LTCM, Enron and Arthur Andersen, the Millennium bug, 9/11, SARS and other near pandemics, even the ash cloud from the Eyjafjallajökul volcano, you will see that they are essentially operational risk events." Simon Ashby, David Clark, John Thirlwell, *Waking the sleeping giant – maximising the potential of operational risk management in banks*, Journal of Financial Transformation, vol 33 (Capco Institute, November 2011)

OPERATIONAL RISK GOVERNANCE

Like a castle, sound operational risk governance relies on multiple lines of defence. These include:

1. business line management
2. independent corporate operational risk management function
3. independent review



The first line of defence is business line management, who should be responsible for identifying and managing the risks inherent in the products, activities, processes and systems for which it is accountable.

The second line of defence is a functionally independent corporate operational risk function whose responsibilities include operational risk measurement and reporting processes, risk committees and responsibility for board reporting. The operational risk function is there to challenge the business line's engagement with the bank's risk management, measurement and reporting systems and to build the overall OR framework. This collection and analysis of data is one of the opportunities for delivering benefit to the business beyond the straightforward risk management - more on that later.

Finally, the third line of defence should be an independent review and challenge of the bank's operational risk management controls, processes and systems. Those performing these reviews must be competent, fully understanding the business complexities and not involved in the development, implementation and operation of the bank's operational risk management framework. Audit and Compliance both have a major role to play in this area, alongside the OR management.

Because operational risk management is constantly evolving along with the business and regulatory environments, management should ensure that the bank's policies, processes and systems remain sufficiently robust to encompass this moving target. Adequate feedback systems that ensure improvements in operational risk management and that senior management can and will act promptly and appropriately on their warnings, are essential. An example of good practice can be found in the aviation industry where airlines employ people to try and circumvent their security controls to place a dummy bomb on board their aircraft. These exercises are used to expose weaknesses that had not been imagined and one can imagine a similar exercise being useful to banks in identifying areas in which trades could be misrepresented, hidden or falsified.

Operational risk is, of course, not new to the regulatory scene, first being mentioned in the consultation paper for Basel II in 1999. From the Basel Committee's Framework for Internal Control Systems in Banking Organisations (September 1998) and the BIS Core Principles for Effective Banking Supervision (October 2006) to the Core Principles Methodology (October 2006) and the Basel Committee on Banking Supervision (BIS) "Sound Practices for the Management and Supervision of Operational Risk"; a framework for designing operational risk management policies, processes, systems and principles for the industry is well established.

This was taken up in 2006 Basel II Accord and the credit crunch has focused both banks' and supervisors' attention on the need to implement robust operational risk management frameworks.

Operational risk is defined in the Basel II Accord as ***"...the risk of loss resulting from inadequate or failed internal process, people or systems or from external events"***. It is inherent in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management programme, covering the full scope of business from front office to back.

It is, however, the responsibility of the supervisors to ensure that the bank's board of directors and senior management put in place sound operational risk management processes to manage the bank's portfolio of products, activities, processes, and systems.

> *"Risk management generally encompasses the process of identifying risks to the bank, measuring exposures to those risks (where possible), ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on an on-going basis, taking steps to control or mitigate risk exposures and reporting to senior management and the board on the bank's risk exposures and capital positions. Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation. In practice, the two notions are in fact closely related and the distinction between both is less important than achieving the objectives of each."*[1]

[1] BIS, Principles of Sound Management of Operational Risk, June 2011, para. 11.

Depending on the bank's business, complexity and the risk profile of the bank's activities, the degree of formality of how the three lines of defence are implemented will vary. However in all cases a bank's operational risk governance function should be fully integrated into its overall risk management structure. Traditionally this has meant a strong alignment between the measurement of operational risk and the more 'direct' risks such as market (including basis) and credit risk. Given the history in assigning quantitative measures and formulae to the direct risks, banks have normally applied a similar approach to operational risk such as a mixture of Monte Carlo models, historical analysis and scenario planning. The challenge is that while financial markets may indeed move to predictable or at least demonstrably measurable criteria, the factors involved in operational risk are less easy to nail down. A neat formula may well be created to assign $ values to the degree of operational risk to which a business is exposed, however operational risk is far less straight forward and in truth the influence of humans on this area is a key variable that is less easily measured. All the rules in the world will not prevent accidents or more especially a deliberate attempt to circumvent the rules – as has been seen in recently publicised cases involving large global banks such as Societe Generale or UBS.

> ***"It would be a mistake to conclude that the only way to succeed in banking is through ever-greater size and diversity. Indeed, better risk management may be the only truly necessary element of success in banking."***
>
> ***Alan Greenspan, Chairman of the Federal Reserve, American Bankers Association, Annual Convention, October 5, 2004***

This is not to say that quantification is not useful. Any advanced measurement will require metrics in order to put a value to the risk and to allow measurement, as well as recognition of unexpected / expected losses and the use of external data. Naturally a degree of measurement of the wider risks in running a business is important to understand the scale of any shortfall in process. Importantly, over time the collection of this data will also allow a far more accurate understanding of loss tracking and loss patterns, thereby allowing refinement and optimisation of those models. **The key element is in ensuring a wider positive reinforcement process in the management of this risk**.

> ***"... It is not simply that the models employed over recent years – notably Value-At-Risk – make assumptions, such as normally distributed returns, that are manifestly false. It is not just a matter of finding better models, useful though that might be"***
>
> ***Paul Tucker, Deputy Governor of the Bank of England Oct 2012***

To look at two differing examples:
A trader in Bank A discovers an error in an executed trade where the rate was incorrectly entered into the bank system. The error has been discovered by chance and happily the loss is small. He corrects the error, breathes a sigh of relief that he can absorb the loss in his trading book and that nothing serious came of this - and life carries on, no-one is any the wiser.

A flight attendant on a flight from New York to London discovers that the incorrect temperature can be entered into their microwave which delivers food that is dangerously hot. The food is not delivered and a report log is completed and submitted as soon as the flight lands.

The stories above are examples of how two different industries typically approach a discovered operational risk and could hardly deliver a more striking contrast. In Bank A the error is corrected and never mentioned again. No-one learns from the error and an identical mistake could be made by our trader's colleague a few days later, this time for a significant loss. In the airline industry there is an established and robust workflow around reporting any errors – indeed flight attendants are rewarded for discovering and reporting mistakes, including their own.

Through having a policy of open reporting and correction, the outcome is entirely different – errors are driven out of the system and positive behaviour is reinforced. A positive culture for reporting errors and potential errors, rather than only learning from significant negative events should be the aim. Close shaves should not be brushed under the carpet but highlighted as learning points. ***Does the financial industry learn from its mistakes or only from being caught?***

The examples above may be more extreme than most bankers would wish to admit and indeed there is evidence that a cultural shift has already started. Operational Risk is at the heart of business, affecting some 70-80% of the business rather than a token 10% to cover what is left after taking account of the core business risks. The outcome of poor operational risk management can lead to significant core business risks (for example a missed and subsequently discovered trade can result in both market and credit risk).

> ***If you get buy-in you can achieve extraordinary things. But if you do not get buy-in you won't even achieve the ordinary. It's alright to talk about the tone at the top, but I prefer to talk about the tune in the middle. (Sir Mervyn King, Governor of the Bank of England in RSA Sept 2008)***

Strong quantitative measurement is important as a starting point to measure operational risk as far as possible, however many commentators are now emphasising the need for a wider ethos within the company and that the attitude of management to the wider risk has to be driven from board/senior management and then to be carried down actively through the management layers. Indeed the recently published FSB paper on operational risk emphasises how banks should be managing risk beyond quantification due to the potential impact of wider business risks; for instance the bank premises could collapse and notwithstanding an excellent capital base, if there are insufficient disaster recovery facilities in place the bank could be unable to continue to transact its business. Strong risk management is therefore more than simply holding sufficient capital aside to cover the measured risks, it is also having in place the policies and procedures to manage the ongoing business. To put it another way - this is not simply compliance, it is ensuring you stay in business.

> ***"Bankers forgetting or choosing to ignore the fact – as did policy makers – that banks are different, that unlike retailers, or manufacturers, or hoteliers, their failure can have consequences for the whole economy not just their shareholders, and that we therefore need bank boards and management to strike a different balance between risk and return than is appropriate in other sectors of the economy.***
>
> ***So the crisis was not a bolt from the blue – it arose from poor supervision, from bad rules and structures, from dangerous cultures – and the errors were made by regulators, economists, central bankers and public policy makers, as well as bankers themselves. A lot of apparently very clever people got it very wrong, and the ordinary citizen suffered. We have to do better in future."***
>
> ***Lord Turner, Chairman, Financial Services Authority, Mansion House Speech, 11 October 2012***

Considering an analogy to illustrate the ultimate development of operational risk; imagine a doctor treating a patient's wound. An immediate response to the trauma may have been to apply a plaster or band-aid to the wound. Whilst this stops the bleeding by treating the immediate symptom, the underlying wound remains. The doctor treats the wound more permanently by applying stitches and ensuring that the wound will fully heal. The parallel is not simply about plugging a near miss but also speaking up and ensuring that this particular wound is permanently healed. A complete Operational Risk solution could be argued as taking an even deeper approach with management looking to foresee where an injury might occur in the future and to mitigate for that risk before it occurs – preventing the accident and the wound from appearing in the first place.

An example of this preventative approach was seen recently at the London Olympics. Traffic management controls were put in place for people arriving at the major London train stations. By predicting where heavy traffic flow might occur, the potential overcrowding issues were successfully mitigated through established lanes and foot traffic circulation measures that were implemented at certain times of day. The possibility of over-crowding was managed before it became real.

BASEL III

BIS Principles for the Sound Management of Operational Risk

The recent BIS consultation paper on Principles for effective risk data aggregation and risk reporting[2] reveals the increasing focus of the regulators on the importance of this area. This paper makes it clear that for the regulators "*One of the most significant lessons learned from the global financial crisis that began in 2007 was that banks' information technology (IT) and data architectures were inadequate to support the broad management of financial risks. Many banks lacked the ability to aggregate risk exposures and concentrations quickly and accurately at the bank group level, across business lines and between legal entities. Some banks were unable to manage their risks properly because of weak risk data aggregation capabilities and risk reporting practices. This had severe consequences to the banks themselves and the stability of the financial system as a whole*."

The Principles are designed to:

- Enhance the infrastructure for reporting key information, particularly that used by the board and senior management to identify, monitor and manage risks;
- Improve the decision-making process throughout the banking organisation;
- Enhance the management of information across legal entities, while facilitating a comprehensive assessment of risk exposures at the global consolidated level;
- Reduce the probability and severity of losses resulting from risk management weaknesses;
- Improve the speed at which information is available and hence decisions can be made; and
- Improve the organisation's quality of strategic planning and the ability to manage the risk of new products and services.

Bank supervisors believe that these Principles will complement other efforts to improve the intensity and effectiveness of supervision of systemically important financial institutions, particularly in cases where banks do fail. They should also improve risk data aggregation, provide for a smoother, more rapid resolution and reduce the potential recourse to taxpayers. The BIS paper also makes it clear that strong risk management capabilities are, and should be, an integral part of the franchise value of a bank and that there are long-term benefits in improved risk data aggregation capabilities and risk reporting practices which will outweigh the initial investment costs incurred by the banks and other financial institutions to achieve this.
BIS proposes that all regulators should embrace these principles and ensure that by 2016 both global and non-global systemically important banks and other financial institutions meet these standards as well as the other internationally accepted risk management standards[3].

[2] June 2012, http://www.bis.org/publ/bcbs222.pdf.
[3] Principles for the Sound Management of Operational Risk, June 2011, http://www.bis.org/publ/bcbs195.pdf.

Date of issue: December 2012

CONCLUSION

Operational risk is an evolving area which Basel II introduced and which Basel III is ensuring receives increasing attention from all [global] financial institutions. This runs parallel with increased industry awareness and better analysis. Indeed the recently published FSB report highlights both a need for regulators to extend the reach of operational risk management to smaller institutions as well as the need to strengthen capital requirements within this area, given the lower level of sophistication in this area when compared to credit or market risk. Once the preserve of “back office types”, operational risk is now front and centre for the most senior management of many financial institutions as it links with the increasing emphasis on judgment-led supervision and decision-making and not just the creation and use of models to measure risk.

Whilst the cost of controlling operational risk may have risen in recent years, and probably will continue to do so, the related savings from reduced capital allocations are not insignificant – especially in a world where capital will be increasingly scarce and demands on its efficient use will continue to grow. A strong management regime that runs through the very veins of the business will not only ensure a business that is better fitted to survive times of trauma; it will also drive value creation within the business. The opportunity exists not only to act as an 'insurance policy', but also as an area generating recommendations, fed from the collected risk data. An example might be where analysis of call centre data highlights a low response rate in certain circumstances, which negatively impacts customer retention and increases the risk of lawsuits. Improved training and infrastructure, at modest expense, could mitigate this risk and help retain customers. In the ever tighter race to manage business margins, the need for cost savings will turn to the wider business – identifying, understanding and managing potential operational risks will be critical. On the face of it, shaving costs from within the operational risk area may appear to be an easy win, however apart from reducing the possibility of positively managing the business, a failure within this area can be a mission critical decision which threatens the institution itself.

*A central banker recently said **“**You highlight a very important area and one that I've never been comfortable with as a regulator and that is the notion that somehow operational risk can be quantified and capital allocated against it (like credit risk). Most models rely on statistical tools (such as Monte Carlo simulations) or somehow shoehorning qualitative factors into scorecards so that they can be quantified and used as a measure of risk. As you say, it's useful but hardly definitive and the idea that capital can be held to cover unexpected losses caused by failures is nonsense. Experience tells us that in the real world no amount of capital covers catastrophic process failure, a bit like liquidity cannot be covered by capital. **All extra capital does in this circumstance is give you a warm fuzzy comfortable feeling.”***

“The alternatives for regulators are difficult. Personally, I think the whole regulatory environment (Basel III included) is way too pre-occupied with numbers at the expense of the qualitative standards. The problem with qualitative standards is it requires greater skill levels at regulators (which they have to pay for) and is more politically difficult to enforce”

Thomson Reuters

For more information about Thomson Reuter’s key role in market infrastructure and the developing international regulatory framework please contact [robin.poynder@thomsonreuters.com]. Thomson Reuters Marketplaces

For more information
Send us a sales enquiry at
http://thomsonreuters.com/about/contact_us
Read more about our products at
http://thomsonreuters.com/products_services
Find out how to contact your local office
http://thomsonreuters.com/about/locations

Date of issue: December 2012

THOMSON REUTERS™